REMARKS

Claims 1-45 are pending in the application. Claims 1-45 stand rejected by the examiner. Assignee traverses the instant claim rejections.

Examiner's Interview

Assignee's representatives, John Biernacki and Matt Johnson, wish to thank examiner Tamara Teslovich for the courtesies extended during a telephonic interview of June 3, 2009. The interview discussed claim 1 of the application at issue, specifically the use of the term "ephemeral." The remarks and the amendments contained herein further summarize the interview.

Claim Rejections – 35 U.S.C. § 103(a)

On page 3 of the office action, independent claims 1, 16, and 31 are rejected under 35 U.S.C. § 103(a) as being unpatentable over Schneier (U.S. Patent No. 5,956,404) in view of the Perez memo. In rejecting the independent claims, the office action cites to the Background section of the Schneier reference, specifically at column 1, lines 28-65, as teaching encrypting a plaintext message into a ciphertext message, the encrypting step including producing an *ephemeral* key pair that is used to encrypt the plaintext message and generating a digital signature for the ciphertext message using an *ephemeral* key pair, where the *ephemeral* key pair used in the encrypting and generating steps is used for a single message between the sender and the receiver. The cited portion of Schneier is set forth below:

> The public-private key encryption technique has resolved the above-identified problem. Based on a public-key/private-key key pair, every digital message can be encrypted by any one of the key and decrypted by the other, with the public keys recorded in a public directory, which is publicly accessible, and the private key privately retained. Typically, the sender of the message would go to the public-key directory to look for the receiver's public key. Then the sender would encrypt the message with the receiver's public key, and convey the encrypted message to the receiver. The receiver, upon getting the encrypted message,

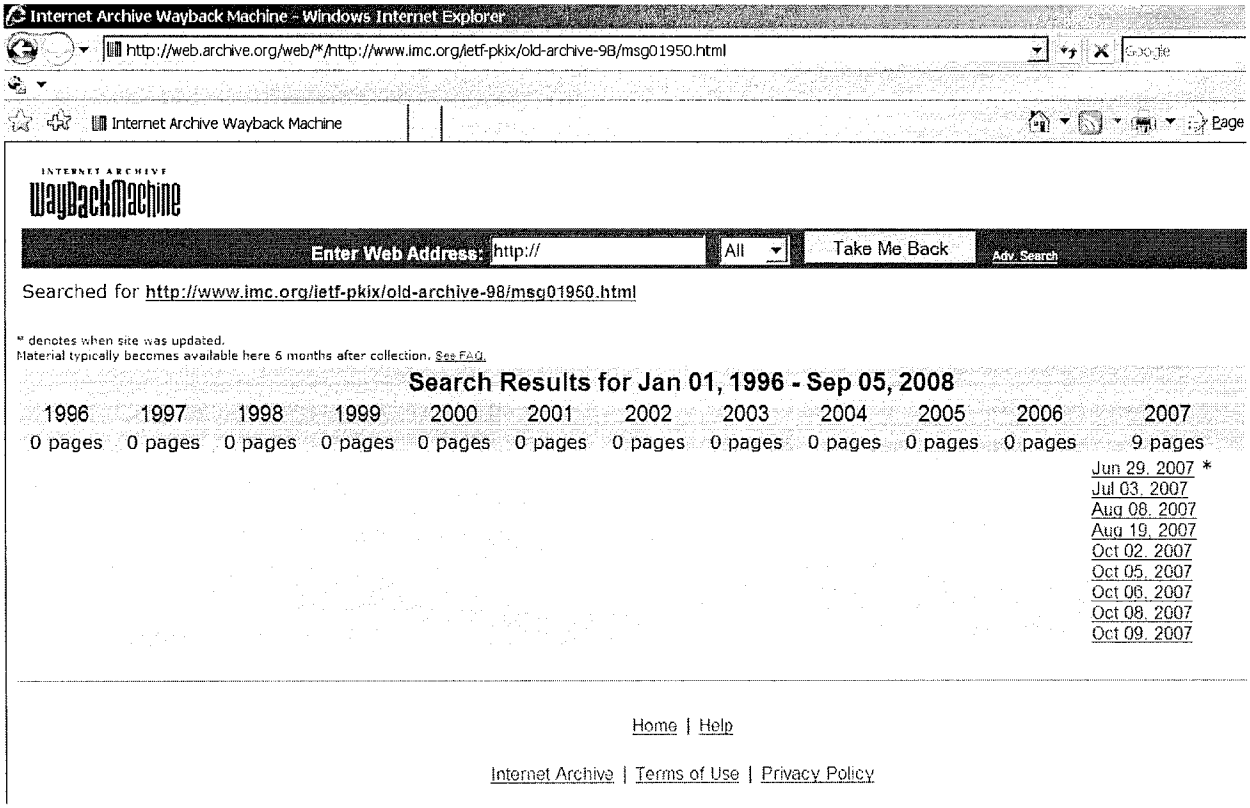
> decrypts the message with her private key. Such a public-private key scheme resolves the problem of maintaining the secrecy of a communication. However, when the receiver gets the message, the receiver cannot be certain that the message is from the sender. The receiver would like to have the equivalence of a signature on the message.
>
> The public-private key encryption technique can also be used to generate a digital signature to authenticate the sender. Typically, the sender would hash the message with a one-way hashing function that is publicly known and is an agreed-upon standard, such as published in the newspaper. Hashing a message is a computation applied to a message that collapses the message and transforms it to a unique value--no two messages have the same value. After hashing, the sender would digitally sign the message by encrypting the hashed message with her private key. Both the digital signature and the message will be encrypted by the receiver's public key, and are then sent to the receiver. The receiver, upon getting the information, decrypts it, and extracts the digital signature from it. Then the receiver gets the sender's public key from the public directory to decrypt the digital signature to get back the same message. This operation ensures the identity of the sender because she is the only person who can encrypt the message with her private key. One cryptosystem that allows digital signatures with message-recovery is RSA. There are also ElGamal variants, which allow signing with message recovery.

As can be seen from reading this text, the Background section of Schneier is merely describing prior art encryption and digital signature steps. Lines 28-45 of this text describes the well-known public-private key encryption process discussed in relation to Figure 1 of the present application, and lines 45-65 describes the well-known digital signature process discussed in relation to Figure 2 of the present application.

What is missing from this relied-upon text, however, is any mention at all of producing an "ephemeral" key pair. The key generating steps discussed in Schneier are static key pairs; they are not "ephemeral," or "temporary." In addition, there is no disclosure in this portion of Schneier of producing such an "ephemeral" key pair that is used to encrypt a plaintext message into a ciphertext message, and then subsequently generating a digital signature for the ciphertext message using the same ephemeral key pair that was used to encrypt the plaintext message, where the ephemeral key pair is used for a single message. The office action correctly makes no

allegations of a teaching of a use of the claimed ephemeral key in the Perez memo. Because neither of the cited references teach or suggest the claimed features requiring use of an ephemeral key pair, it is respectfully submitted that the independent claims are allowable over the cited references.

Additionally, it does not appear that the Perez memo is proper prior art for the given §103 rejection. For the Perez memo to be proper prior art, the Perez memo must have been "published," as the term is used in § 102, before to the priority date of the application at issue. It is unclear to the assignee exactly what the Perez memo is. It appears to be an e-mail message to Bob Jueneman from Aram Perez that was later posted on the Internet. A private e-mail message is not a publication for § 102 purposes. A search of the Internet Archive ("www.archive.org") shows that the web page noted in the references cited page of the office action that contains the Perez memo (http://www.imc.org/ietf-pkix/old-archive-98/msg01950.html) was available as of June 29, 2007, clearly after this application's priority date.



Without proof of publication prior to the priority date of the application at issue, it is respectfully submitted that the Perez memo is not proper prior art. Therefore, it is respectfully requested that the § 103 rejections of the claims be withdrawn.

CONCLUSION

For the foregoing reasons, assignee respectfully submits that the pending claims are allowable. Therefore, the examiner is respectfully requested to pass this case to issue.

Respectfully submitted,

By: _____

John V. Biernacki
Reg. No. 40,511
JONES DAY
North Point
901 Lakeside Avenue
Cleveland, Ohio 44114
(216) 586-3939